UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with account identified as mikebatzphotography.smugmug.com that is stored at premises controlled by SmugMug, Inc., 67 E. Evelyn Avenue, Suite 200, Mountain View, CA 94041	Case No. 2:19-MJ-00258

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
See Attachment B	

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

Applicant's signature

Emily Tripp, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and State: Los Angeles, CA

Hon. Paul Abrams, U.S. Magistrate Judge

Printed name and title

AUSA: S. Lara X0427

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as mikebatzphotography.smugmug.com that is within the possession, custody, or control of SmugMug, Inc. (the "PROVIDER"), a company that accepts service of legal process at 67 E. Evelyn Avenue, Suite 200, Mountain View, CA 94041, regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The warrant will be presented to personnel of SmugMug, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other

sophisticated techniques, including to search for known images of child pornography.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, limited to that which occurred on or after April 2013, which is three months before the first text message indicating that BATZ may be involved in the production of child pornography,[5] including:

i. All e-mails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[5] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored, sent, or received by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All folders and files associated with the SUBJECT ACCOUNT, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, the date and time at which each file was sent, and any user-created organizational structure within the SUBJECT ACCOUNT.

iv. All transactional information of all activity of the SUBJECT ACCOUNT described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting, and emails “invites” sent or received via SmugMug, and any contact lists.

v. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber’s

full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made, any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs;

account management logs; and any other information concerning other e-mail or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT; any and all cookies used by any computer or web browser associated with the SUBJECT ACCOUNT, including the IP addresses, dates, and times associated with the recognition of any such cookie.

(I) any other account associated with the cookie(s) associated with the SUBJECT ACCOUNT.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography, namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Any files or records that refer to or depict child pornography, as defined in 18 U.S.C. § 2256(8), or the sexual exploitation of children, including but not limited to documents that refer to the possession, receipt, distribution, production, transmission, reproduction, viewing, sharing, purchasing, downloading, shipment, order, requesting, trade, soliciting, or transaction of any kind, involving child pornography or the sexual exploitation of children.

iii. Any files, records, pictures, or videos tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

iv. Any files or records that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

v. Any and all files or records which are sexually arousing to individuals who are interested in minors. Such material is commonly known as “child erotica” and includes images of children, written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

vi. Any files or records that pertain to accounts with any Internet Service Provider.

vii. Any passwords, encryption keys, and other access devices that may be necessary to access folders and files in the SUBJECT ACCOUNT;

viii. Any communications, files, records, photos, or videos referring to or depicting the solicitation of nude or partially nude images from individuals who may be minors;

ix. Any nude or partially nude images or videos of individuals who may be minors;

x. Any communications, files, records, photos, or videos referring to or depicting the solicitation of sex or sexual acts from individuals who may be minors, including soliciting sex in exchange for money, drug, goods, favors, or any other reason;

xi. Any communications, files, records, photos, or videos referring to or depicting the solicitation of sex or sexual acts from individuals who may be minors;

xii. Any communications, files, records, photos, or videos referring to or depicting sex or sexual acts involving an individual who may be a minor;

b. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the provider shall disclose responsive data by sending it to the following address via US Mail, or to the following email address:

SA Emily Tripp
11000 Wilshire Blvd, Suite 1700
Los Angeles, CA 90024
Office Telephone: 310-996-4235
Office Fax: 310-996-4009
Email: etripp@fbi.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

AFFIDAVIT

I, Emily Tripp, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since March 2016. I am currently assigned to the Los Angeles Field Office where I have been working on the Violent Crimes Against Children Squad since August 2016. I am also assigned to the multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team, as well as the Los Angeles Innocence Lost Task Force. The SAFE Team is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United Sates Code, Section 2251, et seq. I have participated in investigations into child exploitation, child pornography, and sex trafficking involving minors, and I have executed search warrants as part of those investigations. Many of the child exploitation-related investigations have involved the search, processing, and review of electronic and digital devices, including computers. I have received both formal and informal training from the FBI regarding computer-related investigations and computer technology. My formal training includes 21 weeks of formal education at the FBI Academy, where I took classes on writing affidavits and providing evidentiary testimony. I have also received training on the investigation of commercial sexual exploitation of children and juvenile sex trafficking. I have participated in the execution of numerous operations for the

rescue of juvenile victims of human trafficking. During my career as an SA with the FBI, I have participated in numerous investigations involving the sexual exploitation of children facilitated by the use of computers and other electronic devices. Prior to my employment as a SA with the FBI, I was employed as a Child Protective Services Investigator for the Department of Family and Protective Services with the state of Texas. Through both my training and experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children, and how people use the Internet to commit crimes arising from, and related to, the sexual exploitation of children.

2. I make this affidavit in support of an application for a warrant for information associated with the SmugMug account identified by the account name: mikebatzphotography.SmugMug.com (the "SUBJECT ACCOUNT") that is stored at premises controlled by SmugMug, Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 67 E. Evelyn Avenue, Suite 200, Mountain View, CA 94041.[1] The

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in

information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[2] to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

3. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with a SUBJECT ACCOUNT constitutes evidence, contraband, fruits, or instrumentalities of criminal violations

---

which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[2] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents, witnesses, and evidence that members of the investigation have reviewed. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF INVESTIGATION

5. In or around March 2018, law enforcement began investigating a complaint that MIGUEL ANGEL BATZ, JR. ("BATZ") had traded drugs for sexual acts with a minor. Law enforcement interviewed Minor Victim 1 ("MV1") who told law enforcement that BATZ took nude pictures of MV1 when MV1 was 17 years old, and exchanged money and drugs for sex acts even after MV1 told BATZ that MV1 was under 18 years old.

6. On or about May 24, 2018, law enforcement executed a state search and arrest warrant for BATZ and his home and found at least 20 digital devices. I also participated in an interview of BATZ on or about May 24, 2018. On June 20, 2018, I obtained a federal search warrant from the Honorable Patrick J. Walsh, case number 2:18-mj-0192, to search 20 digital devices,

including an iPhone A1549 (the "iPhone") which was in BATZ's possession at the time of his arrest on May 24, 2018. This digital device search warrant is attached hereto as exhibit A and incorporated by reference.

7. On the iPhone, I saw that BATZ and Minor Victim 2 ("MV2") exchanged text messages regarding the price of nude photographs, and referenced the fact that BATZ knew MV2 was not yet 18 years old. The iPhone also contained at least three nude pictures of MV2. In January 2014, BATZ sent text messages to MV2 indicating that BATZ had uploaded MV2's photos to the SUBJECT ACCOUNT.

8. On the iPhone, I saw that the SmugMug application was installed. Using the iPhone, while the iPhone was disconnected from the internet, I could see that local data associated with the SUBJECT ACCOUNT stored on the iPhone included image galleries named after suspected minor victims. For example, fifteen of the locally stored SmugMug galleries associated with the SUBJECT ACCOUNT included the picture and name of Minor Victim 3 ("MV3").

9. Separate from the data associated with the SUBJECT ACCOUNT, the iPhone also contained a video of MV3 having oral sex with a man who I believe to be BATZ. MV3 wore the same outfit in the iPhone video as MV3 wore in a locally stored SmugMug photo associated with the SUBJECT ACCOUNT. I believe the man in the iPhone video performing sex acts with MV3 was BATZ based on my interview with MV3. I also know that MV3 was

17 years old at the time this iPhone video was created because MV3 was still a minor when law enforcement obtained the video.

10. I believe there is probable cause that the SUBJECT ACCOUNT has additional depictions of child pornography and contains evidence that this child pornography was being produced, possessed, and possibly distributed.

III. STATEMENT OF PROBABLE CAUSE

A. LAPD Investigates and Arrests BATZ

11. On or around April 4, 2018, Los Angeles Police Department ("LAPD") Detective Sammy Cruz provide me with a police report which stated that MV1 had met BATZ in 2014. In 2014, BATZ was approximately 32 years old. According to the report, in 2017 BATZ began giving MV1 drugs in exchange for sexual acts. MV1 was a minor at the time.

12. On or about March 27, 2018, LAPD detectives conducted a recorded interview with MV1, which I have reviewed. During the interview, MV1 stated MV1 had met BATZ, and BATZ told MV1 that BATZ was a photographer. BATZ told MV1 that he would give MV1 money if MV1 sent him nude images of MV1. MV1 told BATZ that MV1 was 17 years old and he stated he knew how old MV1 was, and continued to ask for the nude pictures. MV1 sent BATZ nude pictures in exchange for money. Later, BATZ met MV1 in person to exchange money for sex acts while MV1 was still a minor.

13. MV1 identified BATZ's Instagram name to law enforcement and provided law enforcement with permission to search MV1's cell phone. On April 2, 2018, law enforcement searched MV1's cell phone and discovered an Instagram direct

message chat conversations on or around December 5, 2017, where BATZ offered to pay MV1 for nude videos. BATZ directed MV1 on what he wants in the videos and how much he will pay. On or around December 10, 2017, MV1 sent BATZ an Instagram message where she told BATZ that she was 17 years old. BATZ responded, in part, "I assumed you were cause of the age you were when we first shot. I'm fine with it." MV1 told law enforcement that she met up with BATZ to perform sexual acts in December 2017, and February 2018.

14. On May 24, 2018, I was present when LAPD executed a search and arrest warrant for BATZ and his residence. LAPD seized at least 20 digital devices, including the iPhone which was on BATZ's person. BATZ was arrested for a violation of California Penal Code Section 288a(b)(1), Oral Copulation of a Minor. I was also present at an interview with BATZ and can recognize his voice.

15. On June 20, 2018, the Honorable Patrick J. Walsh signed a federal search warrant to search the 20 digital devices, including the iPhone. This search warrant is attached hereto as Exhibit A, and is incorporated by reference. This search warrant authorized a search of, among other things, data, photographs, videos, and applications stored on the iPhone. On or about October 17, 2018, law enforcement obtained an extension of time to search the iPhone.

B. BATZ's iPhone Contains Messages About Child Exploitation

16. In or about November 2018, I searched the files and data locally stored on the iPhone. At the time of the search, the iPhone was disconnected from the internet and could not access any outside servers. During this search, I discovered that the iPhone had the SmugMug application[3] installed. As discussed in further detail below, SmugMug and the SUBJECT ACCOUNT on SmugMug were referenced in BATZ's conversations with MV2.

17. In the iPhone, I found and reviewed text messages between BATZ and MV2, including the following exchange:

a. On or around November 10, 2013 BATZ and MV2 discussed arranging a "one on one" photo shoot, and asking if MV2 is willing to do full nude photos "like last time." MV2 responded that MV2 would do full nude photos for the same price as last time, $150 for the last hour, or just topless photos for $90.

18. In the iPhone, I found three pictures of MV2 nude seated on a couch facing the camera with MV2's vaginal area exposed. Based on the metadata in these pictures, these pictures were taken in or about July 2013.

19. Through further investigation, I discovered MV2's identity and obtained MV2's California Department of Motor Vehicles ("DMV") records. Through these records I confirmed

[3] SmugMug is a photo gallery application, mainly used by photographers, to securely store, share, or sell photographs to others.

that MV2 was 17 years old on November 10, 2013. I also obtained MV2's DMV photo and visually confirmed that MV2 was the person in the three nude iPhone pictures.

20. On November 11, 2013, BATZ texted MV2 and wrote, "Hey when you turn 18 are you gonna publicly post your topless pics? If you plan to, I will hold on to the ones we shot yesterday and edit them for you when you turn 18 cause there's a couple that are really artistic looking in black and white."

21. On or about December 5, 2013, BATZ offered MV2 $125 plus marijuana for a nude photo shoot. MV2 agreed but stated "im not like spreading my lips or anything just artistic nude." BATZ replied, "but that's what I wanted, you used to send me some sexy pics I wanted to shoot some of my own."

22. On or about January 26, 2014, BATZ sent MV2 a text message saying that he had completed editing MV2's photos and he will upload them to SmugMug. On or around January 31, 2014, BATZ sent MV2 a link to the SUBJECT ACCOUNT.

23. In the iPhone, I also discovered numerous text messages to different people which included links to the SUBJECT ACCOUNT. I noticed that typically the SUBJECT ACCOUNT links were for galleries which match the name of the women in the text messages. I have not yet identified all of these individuals or whether they were all minors when the pictures were taken.

24. On November 6, 2018, I reviewed the locally stored data associated with the SmugMug application on the iPhone. The iPhone was not connected to the internet or any outside servers when I was reviewing this data. Thus, when reviewing this data,

I was only able to view locally stored data on the iPhone. Meaning I could only see the content from the SUBJECT ACCOUNT which was downloaded to the iPhone and available when not connected to the internet. I was unable to view the portion of the SUBJECT ACCOUNT which was not downloaded onto the iPhone. To view the remaining portion of the SUBJECT ACCOUNT, this search warrant is necessary.

25. In my review, I saw that the SUBJECT ACCOUNT contained multiple galleries bearing different female names. Each gallery had a picture of a woman I believe BATZ had photographed and uploaded, based on text message conversations corresponding to the names of some of the galleries. Some of the females in the gallery profile pictures were nearly nude, nude, topless, or bottomless. I have confirmed that at least one of the women, MV3, depicted in these galleries was a minor.

26. Approximately 15 galleries in the SUBJECT ACCOUNT bore a picture of MV3. One of the galleries with MV3's name was marked private. The private gallery had a profile picture of MV3 in a white t-shirt cut to expose the abdomen and lower portion of her breasts and black thong underwear. I recognized the pictures on the SUBJECT ACCOUNT as matching pictures saved in the iPhone where MV3 was wearing what appeared to be the same outfit. The metadata for the matching picture on the iPhone indicated that the photos were taken on April 22, 2018.

27. The iPhone also contained a series videos of MV3 in the same white t-shirt and black thong where MV3 appears to be

performing sexual acts on BATZ. These videos were stored separately from the SmugMug application on the iPhone.

28. In one of these videos, MV3 is nude and appears to manually stimulating BATZ's erect penis. In the video, the man sounds like BATZ and asks MV3 why MV3 has oral sex with other "random guys." MV3 replied that she is upset because BATZ had given more money to the girl BATZ "got in trouble with."[4] BATZ replied that he had given MV1 the "first time rate" which he had also given to MV3. In the next video, MV3 can be seen orally copulating a man's penis. The metadata for both videos indicate that they were filmed on or around April 22, 2018.

29. On December 20, 2018, I spoke to MV3 and confirmed that she was still 17 years old in May 2018, when law enforcement obtained BATZ's phone. MV3 also admitted that she had performed sexual acts with BATZ, and that BATZ had filmed her.

30. A 90-day preservation letter was sent for the SUBJECT ACCOUNT on November 7, 2018 pursuant to 18 U.S.C. § 2703(f). Therefore, I believe there is probable cause that the SUBJECT ACCOUNT contains evidence of criminal activity, in violation of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography.

[4] Based on the context of this video, and previous text conversations between BATZ and MV3, I believe MV3 is referencing BATZ's arrangement with MV1.

31. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the SUBJECT ACCOUNT by other means.

IV. BACKGROUND ON CLOUD SERVICES, E-MAIL, SOCIAL MEDIA ACCOUNTS AND THE PROVIDER

28. In my training and experience, I have learned that providers of e-mail and social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. I have learned that there are numerous cloud-based storage services available for consumers offering many different capabilities. In general, cloud-based storage services can be defined as an online storage medium on the Internet accessed from a computer or electronic storage device. Providers, such as SmugMug, Inc., make it possible for the user to have access to saved files, data, programs, etcetera (referred to as “contents”) without the requirement of storing said contents on their own computers or other electronic storage devices; to include physical hard drives, USB drives, CDS, DVDS, etc. The PROVIDER provides an “offsite” storage medium for contents that can be viewed at any time from any device capable of accessing the Internet.

29. Users can store their contents on a cloud-based storage and avoid having the contents accessed and, in some

cases, appear on their computers. Anyone conducting a search of an individual's computer would not be able to see the contents if the user opted to store the contents in the "cloud." These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

30. In my training and experience, I know that users of cloud-based storage like the PROVIDER can access and sometimes locally store contents also stored by the PROVIDER. Often, when contents are locally stored on a device by a user, the user can access that locally stored content even when offline or without any access to any network.

31. In my training and experience, the subscriber information collected by the PROVIDER during the account registration process - such as name, address, telephone numbers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number) - may constitute evidence of crimes under investigation because the information can identify the user(s) of the SUBJECT ACCOUNT.

32. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in

subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

32. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

33. A subscriber of the PROVIDER can also store with the PROVIDER files in addition other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

34. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or

closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

35. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

36. I request that the PROVIDER provide the entire contents for the SUBJECT ACCOUNT since inception until the time the requested warrant is served on them, and that the items to be seized set forth in detail in Attachment B permit law enforcement to seize such items without limit as to time in

order to assist in identifying the individual(s) participating in the possession, receipt, distribution, and production of child pornography. I further request this because the SUBJECT ACCOUNT may have historical information about the identities of the user(s) of one or other accounts involved in this crime. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion

and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

37. Providers of similar services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI (Uniform Resource Locator or Indicator, i.e., a website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT. These can be used to determine the types of devices used while accessing the SUBJECT ACCOUNT, as well as data related to the user's activity while accessing the SUBJECT ACCOUNT.

38. I have also learned that providers of e-mail and social media services often track the behavior and activities of persons using accounts by using cookies, which are strings of characters and numbers stored on a person's computer on their

web browser. These cookies can often show whether more than one account was accessed by the same computer (and specifically the same web browser), as the provider can recognize that cookie when the same device returns to the service to access an account.

39. In order to identify other accounts used or maintained by the user of a SUBJECT ACCOUNT, the warrant also calls for the PROVIDER to disclose both (1) any cookies associated with the SUBJECT ACCOUNT, i.e., those cookies that were placed on any computers or web browsers (for example, Internet Explorer or Google Chrome) used to access the SUBJECT ACCOUNT, and (2) the identity of any other account in which the same cookie or cookies used to access the SUBJECT ACCOUNT was/were recognized. If in the course of the investigation the digital devices used by the subject(s) of the investigation are found, they can be searched to determine if the cookies recognized by the provider are stored on those devices. The warrant also calls for the PROVIDER to identify any other accounts accessed by any computer or web browser using the same cookies as the SUBJECT ACCOUNT by providing subscriber records and log-in information for those other accounts (but not to provide the contents of communications in those other accounts).

40. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the

misleading impression that only a single user had access to the account.

41. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. “Keyword searches” would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

42. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

43. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore,

would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

V. CONCLUSION

44. Based on the foregoing, I request that the Court issue the requested warrant.

Emily Tripp, Special Agent
Federal Bureau of
Investigations

Subscribed to and sworn before
me on January ___, 2019.

HONORABLE PAUL L. ABRAMS
UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 04/12/13)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
SUBJECT DEVICES 1-20 AS IDENTIFIED IN ATTACH. A THAT WERE SEIZED ON 5/24/2018, AND PRESENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION IN LOS ANGELES, CALIFORNIA.

Case No. 2: 18-MJ-1592

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(a), (e); 2252A(a)(2)(A), (b)(1); 2433(b)	Attempted production and receipt of child pornography. Enticement

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Emily Tripp, FBI SA
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/20/18

Judge's signature

City and state: Los Angeles, California

Honorable Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Jennifer Chou/sb (213) 894-6482/6.20.18

AFFIDAVIT

I, Emily Tripp, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since March 2016. I am currently assigned to the Los Angeles Field Office where I have been working on the Violent Crimes Against Children Squad since August 2016. I am assigned to the multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team, as well as the Los Angeles Innocence Lost Task Force. The SAFE Team is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United Sates Code, Section 2251, et seq. I have participated in child pornography investigations and executions of search warrants concerning those offenders. I currently investigate criminal violations relating to child exploitation and sex trafficking involving minors. During my employment as an SA, I received 21 weeks of formal education at the FBI Academy, which included instruction in writing affidavits and providing evidentiary testimony. I have also received training on the investigation of commercial sexual exploitation of children and juvenile sex trafficking. I have participated in the execution of numerous operations for the rescue of juvenile victims of human trafficking. Prior to my employment as an SA with the FBI, I was employed as a Child Protective Services Investigator for the Department of Family and Protective Services with the state of

Texas. In this capacity, I investigated allegations of abuse and neglect of children including sexual abuse of minor victims, analyzed information, and implemented appropriate actions to reduce the threat of safety to a child. I have received both formal and informal training from the FBI and other institutions regarding crimes against children. Through both my training and experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children, and how people use the Internet to commit crimes arising from, and related to, the sexual exploitation of children.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant to search the following digital devices in the custody of the FBI:

a. One gray Lenovo laptop 120S-14IAP, model name 81A5, bearing serial number YD03RAWW ("SUBJECT DEVICE 1");

b. One gray Dell Inspiron laptop, model number PP20L, bearing serial number (01)07898349891747 ("SUBJECT DEVICE 2");

c. One black HP computer, model TPC-F025-SF, bearing serial number MXL2380LKR ("SUBJECT DEVICE 3");

d. One black Toshiba hard drive, bearing serial number 64DATZX4T18B, 2TB capacity ("SUBJECT DEVICE 4");

e. One black Toshiba hard drive, bearing serial number 28LBTZVBT10F, 1TB capacity ("SUBJECT DEVICE 5");

f. One black Toshiba hard drive, model number HDDR320E03X, bearing serial number 58LST2GDTC73, 320GB capacity ("SUBJECT DEVICE 6");

g. One white Nikon Camera, model Coolpix S33, bearing serial number 30110184, 25MB internal storage ("SUBJECT DEVICE 7");

h. One black Canon camera, model number EOS 5D Mark III, bearing serial number 332022001369 with internal storage capability ("SUBJECT DEVICE 8");

i. One black Canon camcorder, bearing serial number 422250100022, 32GB internal storage ("SUBJECT DEVICE 9");

j. One Panasonic camcorder, bearing model number PV-GS80 ("SUBJECT DEVICE 10");

k. Two Sony premium mini digital video cassettes, each bearing model marking numbers 04HC2304H 1714 ("SUBJECT DEVICE 11" and "SUBJECT DEVICE 12," respectively);

l. One 16 GB Lexar Platinum II SD Card, recovered from SUBJECT DEVICE 7 ("SUBJECT DEVICE 13");

m. One T-Mobile SIM card, bearing Integrated Circuit Card Identifier ("ICCID") 260410029431705 ("SUBJECT DEVICE 14");

n. Approximately 180 miscellaneous compact discs consisting of CDs and DVDs (collectively, "SUBJECT DEVICE 15");

o. One 16GB San Disk Ultra SD card, recovered from SUBJECT DEVICE 8 ("SUBJECT DEVICE 16");

p. Three 16GB San Disk Ultra SD Cards, recovered from a desk drawer (collectively, "SUBJECT DEVICE 17");

q. One black iPhone 5 cellular telephone, bearing model number A1426 and International Mobile Equipment Identity ("IMEI") 013333006462394 ("SUBJECT DEVICE 18");

r. One black Alcatel cellular telephone, bearing model number 5065N and IMEI 014705000643203 ("SUBJECT DEVICE 19");

s. One silver iPhone 5 cellular telephone, bearing model number A1549 and IMEI 356986067061788 ("SUBJECT DEVICE 20");

t. One mini digital video cassette, bearing model marking number 53HC4407E 0929, which is inside SUBJEECT DEVICE 10, the Panasonic camcorder ("SUBJECT DEVICE 21")[1] (collectively, the "SUBJECT DEVICES").

3. This affidavit is also made in support of an order to authorize law enforcement to depress Miguel Angel Batz, Jr. ("BATZ")'s fingerprints and/or thumbprints onto SUBJECT DEVICES 18 and 20, the two iPhone cellular phones.

4. The requested search warrant seeks authorization to seize any data on the SUBJECT DEVICES that constitutes evidence or fruits of violations of 18 U.S.C. § 2251(a), (e): attempted production of child pornography; 18 U.S.C. §§ 2252A(a)(2)(A), (b)(1): attempted receipt of child pornography; 18 U.S.C. § 2433(b): enticement (collectively, the "Subject Offenses"), and any SUBJECT DEVICE which is itself or which contains

[1] The camcorder, SUBJECT DEVICE 10, must be powered on in order to eject the tape, SUBJECT DEVICE 21. I am currently attempting to obtain a power cord for SUBJECT DEVICE 10.

evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

5. The SUBJECT DEVICES are identified in Attachment A to the search warrant application. The list of items to be seized is set forth in Attachment B to the search warrant application. Attachments A and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. DEFINITION OF TERMS

7. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256.

b. "Child erotica" means materials or items that are sexually arousing to persons who have a sexual interest in minors, but that are not, in and of themselves, legally obscene, or do not necessarily depict minors in sexually explicit conduct.

c. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

d. The term "email" (electronic mail) is defined as the text messages sent from one person to another via a computer. Email can also be sent automatically to a large number of addresses via a mailing list.

e. The term "Internet" is defined as the worldwide network of computers — a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

f. "Computer Server" or "Server" is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol address

so the computer hosting the website may be located, and the DNS server provides this function.

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer software" or "software" is digital information which can be interpreted by a computer or any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a

digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

k. The term "IP Address" is defined as a unique number assigned to each computer directly connected to the Internet (for example, 172.191.142.150). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

i. There are two versions of IP: IPv4 and IPv6.

ii. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^{32} addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will

eventually run out because every device — including computers, smartphones and game consoles — that connects to the Internet requires an address.

iii. The difference between IPv6 and IPv4 IP Addresses: An IP address is a sequence of binary numbers that can be stored as text for human readers. IPv4 are a 32-bit numeric sequence written in decimal form as four numbers - zero to 255 - separated by periods. For example, 1.160.10.240 could be an IPv4 address. IPv6 addresses are 128-bit IP address written in hexadecimal form and separated by colons. For example, 3ffe:1900:4545:3:200:f8ff:fe21:67cf could be an IPv6 address. An assigned account may have multiple IP addresses, but each unique IP address relates back to only one Internet account.

l. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

m. The term "open source" is defined as software that includes a free license; in other words, it is freely available to everyone using the Internet.

n. The terms "jpeg," "jpg," "gif," "bmp," and "art" are defined as graphic image files, namely, pictures.

o. The terms "mpeg," "mpg," "mov," "avi," "rm," and "wmv" are defined as video or movie files. To use these video files, one needs a personal computer or other digital device with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

p. "Hyperlink" refers to an item on a webpage which, when selected, transfers the user directly to another location in a hypertext document or to some other webpage.

q. "Chat" means any kind of communication over the Internet that consists of the real-time transmission of messages between two users. Chat messages enable participants to respond quickly to one another and in a format that is similar to an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and e-mail.

8. "Cloud-based" Storage Services or "Cloud Account(s)" are widely available for consumers offering many different capabilities. Dropbox.com ("Dropbox") is a cloud-based digital storage service. In general, cloud-based storage services can be defined as an online storage medium on the Internet accessed from a computer or electronic storage device. The Providers (companies offering this service) make it possible for the user

to have access to saved files, data, programs, etcetera (referred to as "contents") without the requirement of storing said contents on their own computers or other electronic storage devices; to include physical hard drives, USB drives, CDS, DVDS, etc. PROVIDERS provide an "offsite" storage medium for contents that can be viewed at any time from any device capable of accessing the Internet. Users can store their contents on a cloud-based storage and avoid having the contents accessed and in some cases appear on their computer. Anyone conducting a search of an individual's computer would not be able to see the contents if the user opted to store the contents in the "cloud." These are often viewed as advantageous for collectors or child pornography in that they can enjoy an added level of anonymity and security.

IV. STATEMENT OF PROBABLE CAUSE

9. As described further below, the SUBJECT DEVICES were seized during the execution of a California state search warrant[2] from the residence, vehicle, business, and person of BATZ, whom law enforcement believes solicited minor victims for child pornography.

10. On or around April 4, 2018, the Los Angeles Police Department ("LAPD") Detective Sammy Cruz, who is with the Detective Support and Vice Division - Human Trafficking Unit, provided me with a report regarding the LAPD's investigation of BATZ. From my review of the report, I learned the following:

[2] A redacted copy of the state search warrant (but not the addenda to that affidavit) is attached at Attachment C and is hereby incorporated by reference.

a. On March 1, 2018, Detective Cruz received a Cyber Tip that BATZ had met a minor female victim ("MV1") on Instagram in 2014, then subsequently introduced MV1 to drugs and provided MV1 with drugs in exchange for sexual acts. In 2014, BATZ was approximately 32 years old, and MV1 was approximately 14 years old.

b. On March 12, 2018, Detective Cruz met with MV1's mother. MV1's mother told Detective Cruz that she had observed text messages between BATZ and MV1 that contained nude photos and videos MV1. MV1's mother provided MV1's cell phone to the LAPD and gave verbal consent for law enforcement to search the phone.

11. On March 27, 2018, MV1 was interviewed by Detective Cruz and LAPD Detective Aaron Korth. The interview was recorded. I have listened to the audio recording of this interview and learned the following:

a. MV1 said that she met BATZ during a photography shoot in Santa Monica when MV1 was 14 years old. BATZ knew she was 14 years old at the time. BATZ messaged MV1 a couple of times over the next few years. MV1 ignored BATZ's messages until approximately September or October 2017. At that time, MV1 had a drug problem and needed money. BATZ offered to pay MV1 money in exchange for nude videos and photos of MV1. MV1 told BATZ she was 17 years old. BATZ said that he knew how old she was.

b. MV1 said they met in December 2017 at a residence that BATZ said was his parents' house. There, BATZ photographed

MV1 in lingerie and told her he would pay her more money for nude photos of herself. MV1 stated BATZ then took photos and video of her naked and gave MV1 $200 dollars in exchange.

c. MV1 said that she met BATZ a second time at the same residence, where she gave BATZ a hand job, which he videotaped, and then he gave her $400 to $500.

d. MV1 said she met BATZ a third time, around the end of February, when BATZ picked up MV1 from her home. She orally copulated BATZ in the car and BATZ gave her money and alcohol.

e. MV1 said that BATZ told her he had met up with another girl she knew from school. MV1 had heard that this other girl had been in trouble at school for being on a "sugar daddy website." MV1 did not know any further details about BATZ involvement with the other girl.

f. BATZ also told MV1 he would get paid to set up other 17-year-old girls for photo shoots with other photographers where "they would do more," which I understand to refer to other sexual activities. BATZ said he had sold sexually-explicit videos of other girls.

g. BATZ also said he used photographs he had taken of other girls for "profile pictures" of fake social media accounts he created. He then used these fake social media accounts to meet other users and "lead guys on" to exploit money from them.

h. MV1 said BATZ had provided MV1 with his Dropbox account's login information so that she could upload sexually

explicit photos and videos of herself to BATZ's Dropbox account in exchange for money.

i. MV1 said that her communication with BATZ was primarily through Instagram messaging and text messages.

12. On March 27, 2018, MV1 gave LAPD written consent to search her cell phone.[3] On April 2, 2018, LAPD searched the cell phone and extracted digital copies of data from the cell phone. I have reviewed the digital extractions from MV1's cell phone.

a. The extractions included screenshots taken of Instagram direct message chat conversations between BATZ and MV1, including a chat conversation that occurred on or around December 5, 2017. This chat conversation included the following:

i. BATZ asked MV1 for a nude video and wrote: "honestly the most I would do is $100 for a 3 minute nude video with you playing with yourself and sucking on your finger."

ii. BATZ commented he was not able to save the videos from direct messaging and told MV1 to download Dropbox from the App Store, then he provided her the account username "aceisgone@yahoo.com" ("BATZ's Dropbox account") and the password "guitar." BATZ instructed MV1 to "try uploading a pic there and tell me when you're done and I'll check. Then I can continue with payment and then you can send the vids."

---

[3] As noted above, MV1's mother had provided MV1's cell phone to LAPD on March 12, 2018. Although MV1's mother also consented to the search of MV1's phone, LAPD did not search MV1's phone until obtaining MV1's written consent to search the phone.

iii. BATZ agreed to send MV1 $50 for a minute and a half video to know that "its legit" and then another $50 for a second video via Paypal. BATZ confirmed MV1's Paypal account to which he would send the money.

iv. MV1 then sent BATZ a screenshot from her phone of the open Dropbox application displaying a thumbnail of a file named "Baby doll.jpg" that appears to depict a female's nude torso from just below the breasts to the navel.

v. After MV1 uploaded the file to BATZ's Dropbox account and sent the confirmation screenshot, BATZ wrote back that he saw the upload and would send the money "right now." BATZ then requested: "Can you please set your phones camera away from you so I can see your full body including your face for the second video?"

vi. BATZ then sent MV1 a screenshot of his phone with information confirming that he had sent $50 to MV1's Paypal account.

b. On or about December 7, 2017, MV1 used Instagram direct messenger to send a video to BATZ. On or about December 9, 2017, BATZ responded that he received the video and sent MV1 the payment. BATZ also wrote to MV1 that he would pay her more money to shoot nude photos of her in person.

c. In an Instagram direct message chat conversation occurring on or about December 10, 2017, MV1 informed BATZ that she was 17 years old in the following exchange:

MV1: Im also 17 so

BATZ: You already showed me everything so [smiling emoji with sweat gland on forehead] But it's ok I'm

not gonna push you to do something you're no comfortable with

MV1: Ok Im just saying fyi

BATZ: I assumed you were cause of the age you were when we first shot. I'm fine with it.

d. The digital extraction data from MV1's phone also included text and multimedia message service ("MMS") conversations, including a message from MV1 on or about February 26, 2018, in which MV1 asked BATZ, who was using phone number (310) 904-3735, for some of the pictures he had previously taken of her. BATZ texted her a picture depicting MV1 in a shirt and skirt kneeling on a bed in a room that I subsequently identified as BATZ's bedroom in BATZ's residence from the search of May 24, 2018, described further below.

13. On or around April 25, 2018, Detective Cruz obtained and served a state search warrant for BATZ's Dropbox account.[4] In response to the warrant, Detective Cruz received data that included multiple videos of a young white female with blonde hair ("MV2"). The videos depict MV2 dancing while wearing a shirt and underwear, both printed with the phrase "Yes Daddy." In the videos, MV2 exposes her naked breasts to the camera.

14. On or around May 9, 2018, through legal process, I requested and obtained Paypal records relating to "Miguel Angel Batz," the phone number (310) 904-3735, which was used by BATZ to exchange text messages with MV1, and the email address

[4] On April 25, 2018, LAPD obtained search warrant number CC18-79259 signed by the Honorable S. Armstead of the Los Angeles County Superior Court for BATZ's Dropbox account.

"aceisgone@yahoo.com," which was BATZ's username for his Dropbox account.

a. The records confirmed that BATZ made two payments to MV1 on December 5, 2017, each for $50; and one payment to MV1 on December 9, 2017, for $100.

b. The records also indicated that on December 5, 2017, BATZ had accessed PayPal from IPv4 address 107.77.228.137; and on December 9, 2017, BATZ had accessed PayPal from IPv4 address 107.77.229.56.

15. On May 23, 2018, LAPD obtained California state search warrant number CC18-79323, signed by the Honorable S. Armstead of the Los Angeles County Superior Court, authorizing the search of BATZ's residence, located at 2937 South Thurman Avenue in Los Angeles, California ("BATZ's residence"); his business, Batz Auto Upholstery, located at 22025 South Avalon Boulevard in Carson, California ("BATZ's business"), and his vehicle, a 1998 Mercedes Benz, California License Plate Number 7JIX304 ("BATZ's vehicle"); as well as a California state arrest warrant for BATZ for violating California Penal Code Section 288a(b)(1) (Oral Copulation of a Minor).

16. LAPD executed the warrants on May 24, 2018. I was present at the arrest and search of BATZ's residence[5] and vehicle. I have also reviewed reports and received information regarding the search of BATZ's business.

[5] During the search of BATZ's residence, I identified BATZ's bedroom as the room depicted in the photograph BATZ sent to MV1 referenced above in paragraph 8.d.

a. SUBJECT DEVICE 20 (the silver iPhone) was seized from BATZ at the time of his arrest.

b. SUBJECT DEVICES 8 and 16 (the Canon camera and the SD card inside the Canon camera) were recovered from the backseat of BATZ's vehicle.

c. SUBJECT DEVICES 1 (Lenovo laptop), 7 (Nikon camera), 10 (Panasonic camcorder), 21 (Sony mini digital video cassette inside the Panasonic camcorder), 11, 12 (two more mini digital video cassettes), 13 (Lexar SD card inside Nikon camera), and 14 (CDs and DVDs) were recovered from inside BATZ's residence. SUBJECT DEVICE 2 (Dell laptop) was recovered from a trash can in the back yard of BATZ's residence.

d. The remaining SUBJECT DEVICES, consisting of cell phones, hard drives, SD cards, and the HP computer, were seized from BATZ's business, along with women's clothing, including the "Yes Daddy" shirt and underpants worn by MV2 in the images referenced above in paragraph 9.

e. BATZ refused to speak with law enforcement and did not provide any passwords or passcodes for the SUBJECT DEVICES, nor did he agree to unlock any devices using his fingerprint or other biometrics.

f. BATZ is being prosecuted in state court and is currently released on bond.

17. On June 13, 2018, LAPD transferred custody of the SUBJECT DEVICES to the custody of the FBI.

V. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

18. As set forth above, BATZ appears to have used digital devices and digital and online storage devices to attempt to produce, solicit, receive, obtain, and possess child pornography files. Based on the facts set forth above, it is my opinion that there is probable cause to believe that BATZ is sexually interested in children and collecting images of the sexual exploitation of children. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who

have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who access hidden and embedded child pornography-related bulletin boards, and other forums such as newsgroups and IRC chatrooms, are typically more experienced child pornography collectors. These individuals likely would have gained knowledge about such forums through online

communications with other individuals who have a sexual interest in children or images of children.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

19. The images of MV1 and MV2 that investigators have reviewed in this case are in a digital format and were stored on a digital cloud-based program. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact disks make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it — simply and securely — so it can be accessed or viewed indefinitely.

20. It is likely that evidence of this access will found in the SUBJECT DEVICES. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, and/or stored on iPods, Blackberries, or cellular telephones.

21. Furthermore, even if BATZ deleted any images of child pornography that he may have possessed or distributed through any of the SUBJECT DEVICES, there is still probable cause to believe that there will be evidence of the illegal activities — that is, the possession and distribution of child pornography — on the SUBJECT DEVICES. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were created, downloaded, obtained, distributed, or viewed can also be recovered, even after the files themselves have been deleted, using readily available forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, and because there is probable cause to believe that BATZ was soliciting, creating, and retaining sexually-explicit digital photographs and videos of MV1 and other minor victims, there is probable cause to believe that evidence of the Subject Offenses will be found on the SUBJECT DEVICES.

VI. BACKGROUND ON USE OF COMPUTERS AND CHILD PORNOGRAPHY

22. Based upon my training and experience in the investigation of child pornography and the Internet, and information related to me by other law enforcement officers involved in the investigation of child pornography generally, I know the following information about the use of computers with child pornography.

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can scan these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, possess and share large numbers of child exploitation images and videos with other Internet users worldwide.

b. Computer users can choose their methods of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a digital media device, etc. (i.e., "locally") or on virtual servers accessible from anywhere with an Internet connection (i.e., "cloud storage"), or on websites.

c. A "hash value" is a numerical identifier for digital data, such as a particular file. It is obtained by using a mathematical function, often called an algorithm. When a hash value is generated for an image file, any other identical image file will have the same hash value. However, if the data is changed, even very slightly (such as the addition or deletion of a single pixel in an image), the hash value will change. Thus, a hash value can be thought of as a "digital fingerprint" for data — if two images have the same hash value, there is an extremely high likelihood that the images are the same.

d. Although a photo's hash cannot be used to re-create an image or identify people or items within an image, it

can be compared with hashes of other photos as a reliable way to match two different copies of the same image. Hash values can be used in a number of ways to assist law enforcement in investigating child exploitation offenses. For example, in conducting forensics on a computer, law enforcement often runs a "hash value comparison" between files on the suspect's computer and a library of hash values of known images and videos suspected to be child pornography.

e. PhotoDNA is a technology developed by Microsoft in conjunction with the National Center for Missing and Exploited Children ("NCMEC"). It calculates a mathematical hash value based on an existing image that contains child pornography. After building up a library of several thousand images, the software can recognize a match anywhere that it is deployed, even if the photo has been altered. The hash does not need to include identifying information, and the original photograph does not have to be given to law enforcement. While it will not identify child pornography images not in its library - and therefore cannot be used to identify new images — it can identify a huge number of photos that are traded online.

23. Through its Cyber Tipline and its work as a clearinghouse for illegal child sexual abuse images reported by U.S. electronic services providers, NCMEC has unique insight into the identified images of child sexual abuse being distributed on the Web. NCMEC uses PhotoDNA to help enable Google and others to compare hashes of the photos on their

services with hashes NCMEC creates of known images of child pornography.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

24. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

25. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital

devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[6] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-

[6] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used,

what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image

file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

h. The requested time to search is needed to allow the imaging and review of the SUBJECT DEVICES, which include the 180 CDs and DVDs, in addition to the 20 other devices.

26. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that

different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

27. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions. I do not know the passcodes of the SUBJECT DEVICES.

28. For these reasons, agents will likely need to use the fingerprints or thumbprints of the user of any fingerprint sensor-enabled device(s) to attempt to gain access to that device to execute this warrant. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint of BATZ, who is released on state court bond and accessible to law enforcement, to access SUBJECT DEVICES 18 and 20. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my

training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

29. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

30. For the reasons described above, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offense will be found on the SUBJECT DEVICES.

/s/
Emily Tripp, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this 20th day of June, 2018.

Patrick J. Walsh
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on May 24, 2018, and currently maintained in the custody of the FBI in Los Angeles, CA:

1. One gray Lenovo laptop 120S-14IAP, model name 81A5, bearing serial number YD03RAWW ("SUBJECT DEVICE 1");

2. One gray Dell Inspiron laptop, model number PP20L, bearing serial number (01)07898349891747 ("SUBJECT DEVICE 2");

3. One black HP computer, model TPC-F025-SF, bearing serial number MXL2380LKR ("SUBJECT DEVICE 3");

4. One black Toshiba hard drive, bearing serial number 64DATZX4T18B, 2TB capacity ("SUBJECT DEVICE 4");

5. One black Toshiba hard drive, bearing serial number 28LBTZVBT10F, 1TB capacity ("SUBJECT DEVICE 5");

6. One black Toshiba hard drive, model number HDDR320E03X, bearing serial number 58LST2GDTC73, 320GB capacity ("SUBJECT DEVICE 6");

7. One white Nikon Camera, model Coolpix S33, bearing serial number 30110184, 25MB internal storage ("SUBJECT DEVICE 7");

8. One black Canon camera, model number EOS 5D Mark III, bearing serial number 332022001369 with internal storage capability ("SUBJECT DEVICE 8");

9. One black Canon camcorder, bearing serial number 422250100022, 32GB internal storage ("SUBJECT DEVICE 9");

10. One Panasonic camcorder, bearing model number PV-GS80 ("SUBJECT DEVICE 10");

11. Two Sony premium mini digital video cassettes, each bearing model marking numbers 04HC2304H 1714 ("SUBJECT DEVICE 11" and "SUBJECT DEVICE 12," respectively);

12. One 16 GB Lexar Platinum II SD Card, recovered from SUBJECT DEVICE 7 ("SUBJECT DEVICE 13");

13. One T-Mobile SIM card, bearing Integrated Circuit Card Identifier ("ICCID") 260410029431705 ("SUBJECT DEVICE 14");

14. Approximately 180 miscellaneous compact discs consisting of CDs and DVDs (collectively, "SUBJECT DEVICE 15");

15. One 16GB San Disk Ultra SD card, recovered from SUBJECT DEVICE 8 ("SUBJECT DEVICE 16");

16. Three 16GB San Disk Ultra SD Cards, recovered from a desk drawer (collectively, "SUBJECT DEVICE 17");

17. One black iPhone 5 cellular telephone, bearing model number A1426 and International Mobile Equipment Identity ("IMEI") 013333006462394 ("SUBJECT DEVICE 18");

18. One black Alcatel cellular telephone, bearing model number 5065N and IMEI 014705000643203 ("SUBJECT DEVICE 19");

19. One silver iPhone 5 cellular telephone, bearing model number A1549 and IMEI 356986067061788 ("SUBJECT DEVICE 20");

20. One mini digital video cassette, bearing model marking number 53HC4407E 0929, which is inside SUBJEECT DEVICE 10, the Panasonic camcorder ("SUBJECT DEVICE 21") (collectively, the "SUBJECT DEVICES").

TARGET SUBJECT TO PROVIDE FINGERPRINTS/THUMBPRINTS TO UNLOCK SUBJECT DEVICES 18 AND 20

For the following Target Subject, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of the person/s described in Attachment A to the fingerprint sensor/s of SUBJECT DEVICES 18 and 20:

MIGUEL ANGEL BATZ, JR.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251(a), (e): attempted production of child pornography; 18 U.S.C. §§ 2252A(a)(2)(A), (b)(1): attempted receipt of child pornography; 18 U.S.C. § 2433(b): enticement (collectively, the "Subject Offenses"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8);

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256(8);

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256(8);

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer or relate to any production, receipt, shipment,

order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, identifying persons transmitting in interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings;

h. Any records, documents, programs, applications, or materials identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to Dropbox, Paypal, or social media programs, including but not limited to Instagram;

j. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider;

k. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 2937 South Thurman Avenue in Los Angeles, California ("BATZ's residence"); Batz Auto Upholstery, located at 22025 South Avalon Boulevard in Carson, California ("BATZ's business"), and a 1998 Mercedes Benz, California License Plate Number 7JIX304 ("BATZ's vehicle");

l. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of SUBJECT DEVICE;

m. Records, documents, programs, applications, materials, and files describing personal information not belonging to Miguel Angel Batz, Jr.;

a. Records, documents, and materials relating to IPv4 address 107.77.228.137 and IPv4 address 107.77.229.56 (the "Suspect IPv4 addresses");

b. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of Victim files to include photographs, videos, e-mails, chat logs, or other files;

c. Records, documents, programs, applications, materials, and files relating to the online social media accounts of any Victim;

d. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

e. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

2. In searching the SUBJECT DEVICE(S) (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE(S) as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool

Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

3. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

4. Law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of MIGUEL ANGEL BATZ, JR., to the fingerprint sensor/s of SUBJECT DEVICES 18 and 20.

ATTACHMENT C

ATTACHMENT C

2018-79303

STATE of CALIFORNIA COUNTY of LOS ANGELES,

RETURN TO SEARCH WARRANT

Peace Officer (Sammy Cruz), being sworn, says that he/she conducted a search pursuant to the Search Warrant described below:

Issuing Magistrate **(Honorable S. Armstead)**

Magistrate's Court : **Superior Court of California, County of Los Angeles, Central, Dept. 40**

Date of Issuance : **(May 23, 2018)** Date of Service : **(May 24, 2018)**

and searched the following **location(s), vehicle(s), and person(s)**:

2937 S Thurman Avenue, Los Angeles, California 90016.

22025 S Avalon Boulevard, Suite B, Carson, Carlifornia 90745

1986 Mercedes Benz, 2 door silver frame with black convertible top, License plate 7JIX304.

Batz, Miguel Angel Jr, Hispanic male, 5 foot 6 inches in height, approximately 260 pounds in weight, with black hair, brown eyes. Date of Birth: January 23, 1982. California Driver's License: D2365544.

FILED
2018 MAY 31 AM 9:08
LOS ANGELES SUPERIOR COURT

and **Seized the Items***

☒ described in the attached and incorporated inventory.

☐ described below :

Please see attached Los Angeles Police Department Property Report bearing DR number 181410881 for items seized during the service of the search warrant.

I further swear that this is a true and detailed account of all the property taken by me pursuant to the search warrant, and the pursuant to Penal Code Sections 1528 and 1536 this property will be retained in my custody, subject to the order of this court or of any other court in which the offense in respect to which the seized property is triable.

(Signature of Affiant)

Sworn to and Subscribed before me this 31 day of MAY, 2018, at 9:04 A.M. / P.M.

(Signature of Magistrate)

Judge of the **Superior Court of California, County of Los Angeles, Central, Dept.** 43

KEVIN STEINER

(Magistrate's Printed Name)

SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES

* List all items seized, including those not specifically listed on the Search Warrant

Los Angeles Police Department

PROPERTY REPORT

Page 1 of 2

IF EVIDENCE CONT., COMPLETE SHADED AREAS ONLY. IF NOT EVID. CONT., COMPLETE ENTIRE FORM.

NARC ☐ FIREARM ☐ SEARCH ☑ MONEY ☐ TOTAL U.S. CURR. BKD. ☐ EVID ☑ NON-EVID ☐ ONLY 1 CATEGORY PER REPORT

IF RELATED TO PREV BKD EVID, USE THAT DR: 18-1410881

DATE AND TIME OF THIS REPORT	DATE PROPERTY BKD.	IF RELATED TO PREVIOUSLY BOOKED EVIDENCE, ORIG. EVID. BKD. TO (IN THIS CASE COMPLETE ENTIRE REPORT)	DATE ORIG. EVID. TAKEN INTO CUSTO
05/25/2018 0720	05/25/2018		05/24/2018

RESIDENCE ADDRESS	ARRESTEE ☐ EVID. CONT. OF ARREST REPORT	DOB	CHARGE / BKD. DR / BKG. #
2937 S Thurman Avenue Los Angeles CA 90016	Batz, Miguel Angel Jr	/[redacted]/1982	CHARGE 288a(b)(1) PC BKD. DR 181410881 BKG. # 5320684

RESIDENCE ADDRESS (BUS. ADDRESS IF VICT. IS BUSINESS)	VICTIM ☐ EVID. CONT. OF PIR (IF NO ARRESTEE)	R - / B -
		R - / B -

RESIDENCE ADDRESS	☐ OWNER OR IF UNKNOWN ☐ FINDER/POSSESSOR	

AREA OR CITY, & DATE CRIME OCCUR.	TYPE OF PREMISES	DEPT. EMPLOYEE IF BOOKED TO	SERIAL NO.	DIVISION	IF FIREARM, CRT CHECKS: AFS YES ☐ NO ☐ NCIC YES ☐ NO ☐

IS THIS STOLEN PROPERTY?	PROBABLE CRIME	☑ FELONY ☐ MISD.	DATE & TIME PROP. FOUND TAKEN INTO POLICE CUSTODY - LOCATION -	RD, OR CITY IF OUTSIDE
☐ YES ☑ NO	288a(b)(1)		05/24/2018 9:00 2937 S Thurman Avenue, Los Angeles	311

IS THIS FOUND PROPERTY?	DATE & TIME FOUND PROPERTY DISCOVERED -LOCATION DISCOVERED-	RD, OR CITY IF OUTSIDE
☐ YES ☑ NO		

INVESTIGATIVE UNIT	PROP. BKD. AT	NOTIFICATIONS - PERSONS & UNITS	CONNECTING REPORTS - TYPE & DR
	Property Div		

CHECKS, CREDIT CARDS, ETC. (CCD, PLUS OVB) FORGERY/AKA DETS/HARBOR DETS., IF THEIR OCCURRENCE

NARCOTICS (GND)

FIREARM (DSVD & R & I, CRIME/PROP. TT SPTR)

EXTRA COPIES TO:

Use of Evidence Continuation: Use only with Arrest Report or, if no Arrest Report, with PIR. Do not use if evidence is related to previously booked evidence. To book evidence, staple this page on top of Arrest Face Sheet (or PIR Face Sheet, if no arrest) and forward with evidence.

1. CIRCUMSTANCES (WHERE FOUND, BY WHOM, HOW MARKED, ETC.) EXPLAIN IF 10.10.00 NOT ISSUED. GIVE RESULTS OF CRT CHECKS ON FIREARMS.
2. ITEMIZE PROPERTY (LIST NARCOTICS FIRST, THEN MONEY, FIREARMS, PROPERTY WITH SERIAL NUMBERS, AND OTHER PROPERTY, IF RELATED TO PREVIOUSLY BKD. EVIDENCE, START WITH NEXT SEQUENTIAL ITEM NUMBER).
3. IS PROPERTY ELIGIBLE FOR IMMEDIATE DISPOSAL? YES ☐ NO ☑ IF YES, LIST ITEM #'S _____. ENSURE AN "EXTRA COPY" IS FORWARDED TO THE PROPERTY DISPOSITION COORDINATOR (PDC) FOR INPUT INTO APIMS. IF PROPERTY IS ELIGIBLE FOR RELEASE, COMPLETE A PROPERTY DISPOSITION/UPDATE REQUEST, FORM 10.06.00, AND FORWARD IT TO THE PDC FOR INPUT INTO APIMS.

ITEM NO.	QUANT.	ARTICLE	SERIAL NO./TYPE TEST OF DRUG	BRAND/DRUG WEIGHT, UNITS	MODEL NO./DRUG TEST RESULT	MISC.-COLOR, SIZE, INSCRIPTION, CALIBER, ETC. IF MULT. ARREST, INCL. NAME/BKG. # FROM WHOM TAKEN

On May 24, 2018, I (Detective Cruz #33314) served a search signed by the Honorable S. Armstead at suspect Miguel Angel Batz Jr's residence (2937 S. Thurman Avenue, Los Angeles, CA 90016), place of work (Batz Auto Upholstery-22025 S. Avalon Boulevard, Carson CA 90745), and vehicle (1998 Mercedes Benz, License Plate Number 7JIX304). I Detective Cruz, Serial Number 33314 recovered item numbers 1 through 14 from the residence. Detective Angulo, Serial Number 32336 recovered item numbers 15 through 21 from the place of work. Detective Viramontes, Serial Number 27829, recovered items number 22 through 25 from the place of work. Detective Rodriguez, Serial Number 35522 item number 26 through 28 recovered from the vehicle. Detective II Magallon, Serial Number 34934, recovered item number 29 from Miguel Angel Batz Jr. at the time of his arrest.

1	1	Laptop	YD03RAWW	Lenovo	YDNOB8202003	Grey-recovered from northeast bedroom on top of black shelf along the west wall.
2	1	Camera		Nikon		White, with Nikon battery, black case, recovered from northeast bedroom closet on top of weights
3	1	SD Card		Lexar Platinum II		16 GB recovered from Nikon camera
4	1	Laptop		Dell Inspiron		Grey-recovered from backyard trashcan
5	1	Camcorder		Panasonic	PV-GS80	Grey-with battery-recovered from southeast bedroom, on top of desk
6	2	Digital Video Cassette		Sony		recovered from southeast bedroom, on top of the desk

Preliminary Drug Test	SUPERVISOR/INVESTIGATING OFFICER TESTING	SERIAL NO.	WITNESSING OFFICER	SERIAL NO.

Search Warrant Info	DATE	ISSUED BY JUDGE	COURT NO.
	05/23/2018	Honorable S. Armstead	

SUPERVISOR APPROVING	SERIAL NO.	10.10.00 ISSUED?	REPORTING EMPLOYEE(S)	SERIAL NO.	DIV.	DETAIL	PERSON REPORTING (SIGNATURE)
MBeall	32430	YES ☑ NO ☐	S. Cruz	33314	DSVD	HTU	X

DATE & TIME REPRODUCED	DIVISION	CLERK

10.01.00 (03/12)

INC # 180524001085

PROPERTY REPORT

DR NO.

ITEM NO.	QUANT.	ARTICLE	SERIAL NO./TYPE TEST OF DRUG	BRAND/DRUG WEIGHT, UNITS	MODEL NO./DRUG TEST RESULT	MISC.-COLOR, SIZE, INSCRIPTION, CALIBER, ETC. IF MULT ARREST, INCL. NAME/BKG. # FROM WHOM TAKEN
7	1	SIM Card		T-Mobile		recovered from southeast bedroom, on top of th desk, inside a toy plastic ball
8	1	Portfolio		Portfolio Evolution		Black-containing pictures, recovered from south east bedroom on top of desk
9	1	Bathing Suit				Black and red, recovered from southeast bedroom closet
10	1	skirt				multi-colored skirt recovered from south-east bedroom, inside dresser drawer
11	1	Compact Disk Case				Black containing misc cd's recovered from southeast bedroom closet
12	1	Compact Disk Case				Black and yellow containing mis cd's recovered from southeast bedroom closet
13	1	TOP RECOVERED WITH ITEM #10				
14	1	Compact Disks				Misc cd's recovered from southeast bedroom on top of the desk
15	1	CPU /Computer	MXL2390LKR	HP	8300P	with power cord-recovered from desk in the downstairs business office
16	3	Hard drives		Toshiba		In black case, recovered from desk in the downstairs business office
17	3	SD Cards		San Disk		16 GB recovered from top of the desk in the downstairs business office
18	2	cords				power cord and usb cord recovered from top of desk in the downstairs business office
19	1	Camcorder	422250100022	Canon		Black-recovered from top of the desk in the downstairs business office
20	1	Cellular telephone		IPhone	A1428	Black recovered from the top of the wood work bench next to east wall of the business.
21	1	Cellular telephone		Alcatel	5065N	black with battery and sim card recovered from right drawer of desk from upstairs office of the business
22	1	jean shorts				recovered from upstairs business office
23	1	shirt				white shirt with "yes daddy" in front recovered from upstairs office of the business
24	1	skirt				white recovered from upstairs office of the business
25	1	shirt				pink with "yes daddy" in front recovered from upstairs office of the business
26	1	Camera		Canon	EOS 5D	recovered from back seat of the vehicle
27	1	SD Card		SanDisk		recovered from inside of Canon EOS 5D
28	1	garage opener/key		Genie		garage opener with misc keys
29	1	Cellular telephone		IPhone	A1549	recovered from the suspect at the time of his arrest.

SW NO. 18-1323

STATE of CALIFORNIA, COUNTY of LOS ANGELES, SEARCH WARRANT and AFFIDAVIT (AFFIDAVIT)

Detective Sammy Cruz, Serial No. 33314, swears under oath that the facts expressed by him/her in the attached and incorporated **Statement of Probable Cause** are true and that based thereon he/she has probable cause to believe and does believe that the articles, property, and persons described below are lawfully seizable pursuant to Penal Code Section 1524 et seq., as indicated below, and are now located at the locations set forth below. Wherefore, Affiant requests that this Search Warrant be issued.

NON-DISCLOSURE REQUESTED:	☐YES ☒NO	**RETURN EXTENSION REQUESTED:**	☐YES ☒NO
PC 1040-1042 SEALING REQUESTED:	☐YES ☒NO	**HOBBS SEALING REQUESTED:**	☐YES ☒NO
PC 1546.2(a) DELAY OF NOTICE REQUESTED:	☐YES ☒NO	**NIGHT SEARCH REQUESTED:**	☐YES ☒NO

(Signature of Affiant)

(SEARCH WARRANT)

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY PEACE OFFICER IN THE COUNTY OF LOS ANGELES: proof by affidavit, having been this day made before me by **Detective Sammy Cruz** that there is probable cause to believe that the property or person described herein may be found at the location(s) set forth herein and that it is lawfully seizable pursuant to Penal Code Section 1524 et seq., as indicated below by "☒"(s), in that:

- ☐ property was stolen or embezzled;
- ☐ property or things were used as the means of committing a felony;
- ☐ property or things are in the possession of any person with the intent to use them as a means of committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their being discovered;
- ☒ property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony;
- ☐ property or things to be seized consist of evidence that tends to show that sexual exploitation of a child, in violation of Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring;
- ☒ there is a warrant to arrest a person;
- ☐ a provider of electronic communication service or remote computing service has records or evidence, as specified in Section 1524.3, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense; or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;
- ☐ property or things to be seized include an item or any evidence that tends to show a violation of Section 3700.5 of the Labor Code, or tends to show that a particular person has violated Section 3700.5 of the Labor Code;

You are Therefore COMMANDED to SEARCH: (premises, vehicles, persons)

See Attached and Incorporated Description Page(s)

For the FOLLOWING PROPERTY, THING(s) or PERSON(s):

See Attached and Incorporated Description Page(s)

AND TO SEIZE IT / THEM IF FOUND and bring it / them forthwith before me, or this court, at the courthouse of this court. This **Search Warrant** and **Affidavit** and attached and incorporated **Statement of Probable Cause** were sworn to as true and subscribed before me on this 20th day of May, **2018, at** 10:27 **A.M. / P.M.** Wherefore, I find probable cause for the issuance of this Search Warrant and do issue it.

NON-DISCLOSURE APPROVED:	☐YES ☒NO	**RETURN EXTENSION APPROVED:**	☐YES ☒NO
PC 1040-1042 SEALING APPROVED:	☐YES ☒NO	**HOBBS SEALING APPROVED:**	☐YES ☒NO
PC 1546.2(a) DELAY OF NOTICE APPROVED:	☐YES ☒NO	**NIGHT SEARCH APPROVED:**	☐YES ☒NO

(Signature of Magistrate) S. ARMSTEAD (Magistrate's Printed Name)

Judge of the Superior Court of California, County of Los Angeles, Dept. 40

SEARCH WARRANT AND AFFIDAVIT

You are Therefore COMMANDED to SEARCH: **(premises, vehicles, persons)**

2937 S Thurman Avenue, Los Angeles, California 90016, within the County and City of Los Angeles.

The location is on the west side of Thurman Avenue, and is the first property north of Boden Street. The property is further described as a one-story residence with white trim, pink colored stucco, white trimmed windows, and a gray roof. The front of the residence faces east and has a black security door. The residence has a small porch and landing.

The residence has a detached garage which is located west of the main residence. The garage door faces southbound onto Boden Street. The address 2937 is painted black on the curb in front of the location.

The search is to include any attics, basements, garages, storage lockers, safes, buildings attached or unattached that are readily accessible to, under the control of or used by the occupants. It is also to include the vehicles parked on the property, adjacent to the property or in the street that are owned by or under the control of any occupants of 2937 S Thurman Avenue, Los Angeles, California 90016.

The search is to include all occupants at the location at the time the search warrant is served including, but not limited to, the below listed person(s).

22025 S Avalon Boulevard, Suite B, Carson, California, 90745, within the county and city of Los Angeles.

The is on the west side of Avalon Boulevard and is the third property south of 220th Street. The property is further described as a multi-unit business building. The building is white metal structure with brown trim and two orange awnings attached to the front of the business. The front of the business faces east and has a glass entrance door.

SEARCH WARRANT AND AFFIDAVIT

There is a large access opening in the front of the business with the address of 22025 posted in black stencils on the wall north of the access opening.
There are parking stalls on the north side of the business building, with additional large openings to the building. A "Batz Auto Upholstery" sign is posted on the north side of the business property.

The search is to include any attics, basements, garages, storage lockers, safes, buildings attached or unattached that are readily accessible to, under the control of or used by the occupants. It is also to include the vehicles parked on the property, adjacent to the property or in the street that are owned by or under the control of any occupants of 2937 S Thurman Avenue, Los Angeles, California 90016.

The search is to include all occupants at the location at the time the search warrant is served including, but not limited to, the below listed person(s).

1986 Mercedes Benz, further described as a 2-door silver frame with black convertible top. License plate number 7JIX304.

SEARCH WARRANT AND AFFIDAVIT

PERSON(S):

Batz, Miguel Angel Jr. further described as a Hispanic male approximately 5 foot 6 inches in height and approximately 230 pounds in weight, with black hair, and brown eyes.
Date of Birth: [redacted] 1982
California Driver's License [redacted]544

For the FOLLOWING PROPERTY, THING(s) or PERSON(s):

1. Based on the foregoing, I respectfully submit that there is probable cause to believe that the following SUBJECT ITEM(S) themselves constitute instrumentalities of the offense and should therefore be seized:

   a. Any digital device capable of storing any "writing", included but not limited to; handwriting, typewriting, printing, Photostatting, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored, as defined by Evidence Code Section 250 of child pornography as defined by California Penal Code Section 311.

   b. Any "writing" that constitutes evidence of child sexual exploitation as defined by California Penal Code Section 311.3.

2. Based on the foregoing, I also respectfully submit that there is probable cause to believe that the following items, which constitute evidence of violations of California Penal Code Section 311, will be found on the SUBJECT ITEM(S). It is requested that the SUBJECT ITEM(S), once seized, be searched for the following items:

SEARCH WARRANT AND AFFIDAVIT

a. Any "writing" which is a visual depiction of minors engaged in sexually explicit conduct as defined in California Penal Code Section 311.

b. Any "writing," pertaining to the possession, production or reproduction, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in California Penal Code Section 311.

c. Any "writing" which is sent with the intent to seduce a minor as defined by California Penal Code Section 288.2.

d. Any "writing" for the purpose of arranging to meet with a minor for the purpose of sexually exploiting the minor as defined by California Penal Code Section 288.3 and 288.4.

e. With respect to any digital devices falling within the scope of the foregoing search categories, or any digital devices containing evidence falling within the scope of the foregoing search categories, records, documents, programs, applications or materials, or the absence of same, sufficient to show the actual user(s) of the digital device.

3. As used in above and below paragraphs the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any digital device and any forensic copies thereof. As used both above and below, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices.

SEARCH WARRANT AND AFFIDAVIT

4. Items in any form via "written" or electronic as per Evidence Code Section 250, that would tend to show dominion and control of the property searched, to include utility bills, Internet service bills, telephone bills, correspondence, rental agreements and other identification documents.

5. Credit card information including but not limited to bills and payment records for Internet service and payments for receiving child pornography.

6. Photographs and/or videotape of the place being searched and its residents, for comparison with images and video recovered relating to the investigation of the sexual exploitation of children.

7. Any "writing" tending to identify the children depicted in such material as described above.

8. Items that would show an unusual interest in children and children activities: These items to include collections of photographs and magazines depicting children.

SEARCH WARRANT AND AFFIDAVIT

STATEMENT OF EXPERTISE:

I, Detective Sammy Cruz, Serial No. 33314, am your affiant. I am currently assigned as a full-time sworn law enforcement officer with the Los Angeles Police Department and I have been so employed for more than 22 years. I am currently assigned to Detective Support and Vice Division, Human Trafficking Unit and working in partnership with the Los Angeles Police Department's Internet Crimes Against Children Task Force (ICAC). I have two years of experience and expertise in Human Trafficking, Pimping, Pandering, Prostitution, and other child sexual-exploitation types of crimes. I am currently assigned part-time to the Los Angeles County Human Trafficking Task Force. One of the tasks of the HTU is to investigate the trafficking of persons for commercial sex by the means of force, fraud or coercion and any sex trafficking of a minor. Other responsibilities include but are not limited to the enforcement of federal criminal statutes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq.

I have previously been assigned to Rampart Detectives and was the primary investigating officer on numerous Sexual Assault and Major Assault Crimes. While assigned to Operations-West Bureau/Registration Enforcement And Compliance Unit, I registered and monitored convicted sex offenders living within the City of Los Angeles.

I have attended Robert Presley Investigative Core Course and Homicide Course. I have also attended the Los Angeles Police Department Detective Investigative Course, Homicide Course, Sexual Assault Course, and Vice Course.

I have responded to and investigated numerous crimes including, domestic violence, assault with a deadly weapon, various sexual assault crimes, and attempt murders. Subsequently, as an HTU investigator, I have investigated human trafficking incidents that involve additional crimes of kidnaping, assault with a deadly weapon, sexual assault, sex with a minor and other sexual exploitation crimes. I have participated in prostitution related investigations/arrests. Such investigations have led to the rescue and recovery of adult and juvenile victims of commercial sexual exploitation.

SEARCH WARRANT AND AFFIDAVIT

I am in daily contact with, and have received training from, subject matter experts in human trafficking, pimping, pandering, prostitution, sexual assaults, and other sexual exploitation crimes. I have also had formal and informal training in the area of evidence collection, specifically relating to human trafficking, pimping, and prostitution. I have testified in numerous court cases leading to successful convictions.

I have received training from subject matter experts in the investigation of crimes against children and child exploitation. I have personally examined digital videos, pictures and computer images depicting children involved in sexual activity with themselves, other children, and adults. I have worked alongside and received training from senior detectives and officers who are trained subject matter experts.

I am in daily contact with experts in the field of computers, Internet investigations, and other child exploitation crimes. I have been trained to recognize the physical characteristics of prepubescent and adolescent children. I have also assisted in the execution of numerous search warrants involving child pornography/child sexual exploitation.

I have received training and am aware that the following characteristics are generally found in varying combinations in people who produce, trade, distribute, or possess images of child pornography: They view children as sexual objects and receive gratification from sexually explicit images of minors. They collect sexually explicit images of minors, which they use for their own sexual gratification and fantasy. They use images as a means of reliving fantasies or actual sexual encounters. They rarely, if ever, dispose of sexually explicit images of minors because the images are treated as valuable possessions.

They store such images in many different formats including photographs, printouts, magazines, videotapes, and many other forms of digital media such as hard drives, diskettes, CDs and/or DVDs, and other storing devices. The images are stored in many different locations such as their home, their vehicle, their work areas, and other areas under their control.

SEARCH WARRANT AND AFFIDAVIT

The images represent a currency among other collectors and are a means of gaining acceptance, status, trust, and psychological support by exchanging, trading, or selling the images to other people with similar interests.

They maintain images of minors with whom they have had sexual contact. If such a person takes a picture of a minor in the nude, there is a high probability that the minor was used to produce sexually explicit images.

I know that suspects will have used the Internet to gain access to children for the purpose of sexual exploitation. I also know, based on my training and experience, that suspects will chat online with other suspects to share their information on the sexual exploitation of children, including where to watch children, how to access children, how to desensitize victims to sexual abuse, how to hide their actions from law enforcement officials, how to store their child pornography, and how to keep the victims from talking about the abuse.

Based on my training and experience, collectors of child pornography generally prefer to store images in electronic format as computer files. The computer's ability to store images in digital format makes a computer an ideal storage area for child pornography. Portable disks can contain thousands of child pornography images. The portable digital media are particularly well suited to conceal images of child pornography.

SEARCH WARRANT AND AFFIDAVIT

STATEMENT OF PROBABLE CAUSE

On March 1, 2018, I received a Cyber Tip Line Report, bearing number 28299234. The report indicated MV1 [redacted] (17-year-old female victim) met Michael Batz (36-year-old male suspect) on Instagram in 2014. Mike introduced MV1 to drugs, getting her addicted to various illegal narcotics. MV1 began trading sexual acts with Mike in exchange for drugs.

Detective Teague received a telephone call from MV1 mother (Angela D.) who disclosed she had her daughter's cellular telephone. Upon reviewing the contents of the cellular telephone, Angela noticed numerous text messages between MV1 and Mike. The text messages contained nude photographs and videos of MV1

On March 12, 2018, Officer Stefani Carson and I, conducted a follow up Angele D. residence. Angela provided us with MV1 cellular telephone number and a scan disk. The scandisk contained information Angela transferred from the cellular telephone.

MV1 was not available to be interviewed at this time.

On March 27, 2018, my partner (A. Korth, Serial Number 33560) and I, met with MV1 to interview her regarding this incident. I explained to MV1 of her right to have a person of the same gender interview her, and a support person present during the interview, which she refused.

MV1 met Mike at the age of 14, when she and [redacted] (sister) were photographed by him somewhere in the city of Santa Monica. For approximately two years, Mike periodically messaged MV1 in attempt to photograph her again. MV1 ignored the messages she received from Mike until approximately September/October of 2017. Mike asked MV1 to send her nude videos of herself in exchange for money. Due to MV1 drug addiction and her need for money, she sent Mike nude pictures and videos of herself to him. The exchange of pictures and videos continued for several months.

SEARCH WARRANT AND AFFIDAVIT

In December of 2017, MV1 and Mike met up for a photo shoot. Mike picked up MV1 at her residence and drove her to an unknown house. During the photo shoot, MV1 wore lingerie and was paid $200 dollars. MV1 did not know the location of the residence, but described the house with a pink exterior. The interior of the house did not have a lot of furnishings. After the photo shoot, Mike offered to pay MV1 more money if she allowed him to photograph her in the nude, and she (MV1 accepted his offer.

During the second photo shoot, also at the pink house, Mike photographed MV1 without any clothing. Mike also recorded MV1 masturbating him until he ejaculated. MV1 believed Mike paid her approximately $400-$500 dollars for this incident.

Sometime in late February of 2018, Mike picked up MV1 at her residence in an older model Mercedes. While driving around, MV1 oral copulated Mike until he ejaculated inside her mouth. After MV1 oral copulated Mike, he gave her money and alcohol. MV1 did not engage in sexual intercourse with Mike, however she sent him numerous nude photographs and videos of herself. Mike provided MV1 with his Dropbox account information, and directed her to login and upload the pictures and videos into his account.

MV1 believed Mike's contact information on her cellular telephone was listed as MB (initials for Mike Batz). While reviewing MV1 cellular telephone, we were unable to locate a listing with the initials of MB. After MV1 manually entered Mike's cellular number (310-904-3735) into her phone, a contact appeared with an emoji of a tornado. MV1 indicated Mike would message her with different numbers, but did not recall what those numbers were.

I directed MV1 to send Mike a text message in my presence using her (MV1 cellular telephone to engage in conversation, but he did not respond.

MV1 disclosed her relationship with Mike to her friend A[redacted], however she did not disclose his identity to her. A[redacted] and MV1 discussed using a dating website to meet men to earn money and support their drug usage. A[redacted] and MV1 did not go through with the dating website because they did not want family and friends finding out what they were doing.

SEARCH WARRANT AND AFFIDAVIT

While in the eighth grade, a friend introduced marijuana to MV1 The marijuana lead MV1 to use ecstasy, cocaine, Xanax, ketamine, acid, and mushrooms. In August of 2017, MV1 recreational drug use became an addiction. MV1 used her Instagram account to meet unknown males, who would send her money in exchange for nude photographs and videos of herself. MV1 did not meet with these males in person.

During a conversation between MV1 and Mike, he disclosed to her he would arrange dates between girls and men. Mike would also send men videos of girls in exchange for money.

Prior to the completion of the interview, I presented an image of a male Hispanic to MV1 MV1 identified the male as Mike Batz.

On April 2, 2018, I conducted a follow-up to the Orange County Regional Computer Forensics Laboratory and conducted a forensic extraction on MV1 cellular telephone.

Through legal process, the following records were obtained from AT&T.

Subscriber Information pertaining to cellular telephone number 310-904-3735.
Financial Liable Party: Miguel Batz
Credit Address: 22025 Avalon Boulevard, Suite B, Carson, California 90745
Customer Since: 10/25/2012
Contact Home Email: BATZAUTO@YAHOO.COM

Billing Party:
Account Number: 337049186660
Billing Address: 22025 Avalon Boulevard, Suite B, Carson, California 90745.

SEARCH WARRANT AND AFFIDAVIT

Through legal process, the following records were obtained from PayPal.

December 5, 2017, at 8:28:18 PM, Instant transfer sent from email address: batzauto@yahoo.com to email address: [redacted]MV1[redacted]gmail.com in the amount of $50.00 USD.

December 5, 2017, at 9:10:41 PM, Instant transfer sent from email address batzauto@yahoo.com to email address [redacted]MV1[redacted]gmail.com, In the amount of $50.00 USD. December 9, 2017, at 08:18:18 PM, Instant transfer sent from email address batzauto@yahoo.com to email address [redacted]MV1[redacted]gmail.com in the amount of $100.00.

Through legal process, the following records were obtained from Dropbox, Inc.
Three deleted videos recovered containing an unknown female White, wearing a short white shirt with blue print "Yes Daddy" in the front, and white underwear with pink print "Yes, Daddy?" in the back. The female is dancing and exposing her breasts. A possible male Hispanic wearing dark clothing appears in the recording.

On April 26, 2018, Detective Futami (Los Angeles Police Department/Gang and Narcotics Division-United Marshals Task Force) conducted surveillance on Mike Batz. Detective Futami observed Mike exit his residence (2937 Thurman Avenue, Los Angeles, CA 90016) enter a 1986 Mercedes Benz (2 door, silver frame, black convertible top, license plate 7JIX304) and drive to his place of work (Batz Auto Upholstery - 22025 Avalon Boulevard, Suite B, Carson, CA 90745).

On May 15, 2018, Detective Futami observed Mike drive (same vehicle listed above) from his place of work to his residence.

SEARCH WARRANT AND AFFIDAVIT

On May 17, 2018, I reviewed the contents of MV1 cellular telephone obtained from the forensic examination. I printed and attached seven pages of text message conversation between telephone numbers (310-463-6552) MV1 and (310-904-3735) Mike, and one photograph of MV1 posing on a bed. During the conversation between Mike and MV1 they discussed meeting arrangements and drug contacts for Xanax. MV1 also asked Mike to send her pictures of their photo shoot. **(This eight page document is hereto attached as Addendum No. 1)**

I also reviewed 93 pages containing Multimedia Messaging Service (MMS) messages between Mike and MV1 which appears to have been done through Instagram. A heading of "mikebatzphotography_ appears on top of each messaging page. During some messages between Mike and MV1 they discuss prices for lingerie and nude photographs. In other messages, MV1 and Mike negotiate prices for various sexual acts. Mike offered MV1 additional money to allow him to record her giving him oral copulation. MV1 informs Mike, she is not comfortable having her face recorded. In another message MV1 discloses to Mike, she is 17 years old. Mike response, "You already showed me everything, Emoji (Happy face with sweat gland on forehead), But it's ok I'm not gonna push you to do something you're not comfortable with" "I assumed you were cause of the age you were when we first shot, I'm fine with it." **(This 93 page document is hereto attached as Addendum No. 2)**

A computer check via Department resources revealed Mike was previously arrested for Disorderly Conduct-Prostitution, Petty Theft, and Driving While License Suspended.

Based upon my training and experience, suspects interested meeting, traveling, attempting to meet, and/or attempting to travel to engage in any sort of sexual activity with a minor, or possessing and distributing child pornography will also collect non-pornographic photos of children, and magazines describing activities that involve children. Some suspects who sexually exploit children will keep photos of the children they have molested as "trophies".

SEARCH WARRANT AND AFFIDAVIT

The magazines are often maintained so that the suspect can utilize the information to aid in the enticement of children. **Searching for these items will assist us in identifying any potential victims of sexual exploitation.**

Based upon my training and experience, I believe there is sufficient probable cause to search 2937 S Thurman Avenue, Los Angeles, California, 90016, and 22025 S Avalon Boulevard, Suite B, Carson, California, 90745, for all forms of digital media based on the fact that suspects who distribute and possess child pornography will often copy and store the images and videos on other forms of digital media. These forms include but are not limited to: USB Thumb Dives, CD's or DVD's, hard drives, cellphones, tablets, and cameras.